

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

---

LINDA FASZCZEWSKI, Individually and On Behalf of  
All Others Similarly Situated,

Plaintiff,

-against-

BLACKBAUD, INC.,

Defendant.

---

### **CLASS ACTION COMPLAINT**

Plaintiff, LINDA FASZCZEWSKI, individually and on behalf of all others similarly situated, makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

1. Plaintiff brings this action against BLACKBAUD, INC. (“BLACKBAUD”) to obtain damages, restitution, and injunctive relief for the Class, as defined below.

### **NATURE OF THE ACTION**

2. BLACKBAUD is a third party vendor that provides Stony Brook University Hospital with cloud -based and data solution services related to Stony Brook’s patient information, communications and fundraising activities. This class action arises out of the May of 2020, ransomware attack and data breach (“Data Breach”) of BLACKBAUD’s systems between February 7 and May 20, 2020, during which hackers acquired a database that manages Stony Brook’s information. The BLACKBAUD data and servers breached contained identifying, sensitive, and Private Information and personal data from patients, including Plaintiff’s. As a result of the Data Breach, Plaintiff and thousands of other Class Member users suffered

ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

3. Additionally, Plaintiff and Class Members' sensitive Private Information, which was entrusted to BLACKBAUD, its officials and agents, was compromised and unlawfully accessed due to the Data Breach. Information compromised in the Data Breach included a copy of a subset of information retained by Blackbaud, including patient's name, date of birth, address/contact information, attending doctor, insurance provider and medical service department.

4. A true and accurate copy of the notice of data breach, dated September 14, 2020, mailed by Stony Brook University Hospital to Plaintiff is attached hereto as Exhibit A.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated, in order to address BLACKBAUD's (a) legally deficient safeguarding of Class Members' Private Information, which it managed, maintained, and secured; (b) failure to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third-party; (c) failure to identify all information that was accessed; and (d) failure to provide Plaintiff and Class Members with any redress for the Data Breach.

### **PARTIES**

6. Plaintiff is a resident and citizen of Cutchogue, Suffolk County, New York.

7. BLACKBAUD is a Delaware corporation with its principal place of business located on Daniel Island, Charleston County, South Carolina.

### **JURISDICTION AND VENUE**

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one

member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds \$5,000,000 exclusive of interest and costs.

9. This Court has personal jurisdiction over this action because Defendant has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District.

10. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claim occurred in this District.

### **FACTUAL STATEMENT**

#### **A. BLACKBAUD's Business**

11. BLACKBAUD holds itself out as the world's leading cloud software company, providing its clients with cloud software, services, expertise, and data intelligence. It is a publicly traded company with clients that include nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them.

12. In 2019, BLACKBAUD reported that it had "45,000 customers located in over 100 countries," with a "total addressable market (TAM)... greater than \$10 billion."

13. BLACKBAUD manages, maintains, and provides cybersecurity for the data obtained by its clients who are, inter alia, schools and non-profit companies, including Stony Brook University Hospital ["SBUH"], which maintained Plaintiff's Private Information.

14. SBUH is a New York State educational corporation and nationally ranked, 695 bed non-profit, research, and academic medical center located in Stony Brook, New York, providing tertiary care for the entire Long Island region.

15. In the ordinary course of doing business, SBUH was required to provide BLACKBAUD with sensitive, personal and private information of its patients, including Plaintiff, that was then stored, maintained, and secured by BLACKBAUD. This information included:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security numbers;
- Credit card account numbers;
- Medical insurance accounts;
- Healthcare information;
- Healthcare provider information

16. In its 2019 Annual Report, BLACKBAUD specifically addressed its known susceptibility to cyberattacks. The report states, in pertinent part:

If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer.

Fundamental to the use of our solutions is the secure collection, storage and transmission of confidential donor and end user data and transaction data, including in our payment services. Despite the network and application security, internal control measures, and physical security procedures we employ to safeguard our systems, we may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data, which may harm our business, reputation and future financial results.

<https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417> (Accessed August 12, 2020).

17. BLACKBAUD's Privacy Policy North America ("Privacy Policy") expressly applies as follows:

At Blackbaud, we are committed to protecting your privacy. This Policy applies to Blackbaud's collection and use of personal data in connection with our marketing and provision of the Blackbaud Solutions, customer support and other services (collectively,

the “Services”), for example if you are a customer, visit the website, interact with us at industry conferences, or work for a current or prospective customer of the Services.

If you’re a constituent, supporter, patient or student of one of our customers, to which we provide the Services, your data will be used in accordance with that customer’s privacy policy. In providing the Services, Blackbaud acts as a service provider and thus, this Policy will not apply to constituents of our customers.

<https://www.blackbaud.com/company/privacy-policy/north-america> (Accessed August 12, 2020).

18. With regard to securing its constituents, including SBUH, BLACKBAUD makes the following representations with regard to the security of personal information:

We restrict access to personal information collected about you at our website to our employees, our affiliates’ employees, those who are otherwise specified in this Policy or others who need to know that information to provide the Services to you or in the course of conducting our business operations or activities. While no website can guarantee exhaustive security, we maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons.

We also advise all Blackbaud employees about their responsibility to protect customer data and we provide them with appropriate guidelines for adhering to our company’s business ethics standards and confidentiality policies. Inside Blackbaud, data is stored in password-controlled servers with limited access.

<https://www.blackbaud.com/company/privacy-policy/north-america> (Accessed August 12, 2020).

19. In connection with SBUH and its patients, BLACKBAUD had additional obligations to secure patient users’ Private Information to comply with the mandates of the Health Information Portability and Accountability Act (HIPAA).

**B. Data Breaches Put Consumers at an Increased Risk of Fraud and Identify Theft**

20. Cyberattacks and data breaches of medical facilities, schools, and non-profit entities are especially problematic because of the disruption they cause to the overall daily lives of patients, students, donors, and other individuals affected by the attack.

21. The United States Government Accountability Office released a report in 2007 regarding data breaches (“GOA Report”) finding that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”

<https://www.gao.gov/new.items/d07737.pdf>

22. There may be a substantial time lag, measured in years, between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

23. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports. <https://www.identitytheft.gov/Steps>

### **C. The Cyberattack and Data Breach**

24. BLACKBAUD maintained Plaintiff and Class Members' Private Information on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health care, schools, and other facilities over the course of recent years, BLACKBAUD did not maintain adequate security of Plaintiff and Class Members' data, to protect against hackers and cyberattacks.

25. According to its own statements, in May of 2020, BLACKBAUD discovered a ransomware attack that attempted to "disrupt business by locking companies out of their own data and servers."

<https://www.blackbaud.com/securityincident> (Accessed August 12, 2020).

26. According to BLACKBAUD'S statements:

After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. The cybercriminal did not access credit card information, bank account information, or social security numbers. Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly... The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.

<https://www.blackbaud.com/securityincident> (Accessed August 12, 2020).

27. Upon information and belief, the ransomware attack began in February of 2020 and continued for approximately three months until it was stopped in May of 2020.

28. BLACKBAUD did not have a sufficient process or policies in place to prevent such cyberattack, which is evident by its own statements that it has “already implemented changes to prevent this specific issue from happening again.”

<https://www.blackbaud.com/securityincident> (Accessed August 12, 2020).

29. Despite having knowledge of the attack since at least May of 2020 [and probably as early as February] BLACKBAUD did not notify SBUH until July 17, 2020 of the compromised data.

30. BLACKBAUD had obligations created by federal law, contracts, industry standards, common law, and privacy representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

31. Plaintiff and Class Members provided their Private Information to SBUH and BLACKBAUD with the reasonable expectation and mutual understanding that both entities would comply with their obligations to keep such Private Information confidential and secure from unauthorized access.

32. On September 14, 2020 SBUH advised Plaintiff:

“On July 17, 2020, Stony Brook received notice that patient information may have been involved in a security incident on Blackbaud’s systems. Blackbaud detected a ransomware attack on its systems in May 2020.” [Exhibit A]

33. With respect to SBUH, “The information that was on the Blackbaud systems affected by this cyberattack may have included your name, date of birth, address/contact information, attending doctor, insurance provider and medical service department.” [Exhibit A]

34. Despite the representation that the data breach “did not involve access to any Stony Brook systems, including medical systems or electronic health records,” SBUH provided the following warning in its breach notification:



“Impacted patients are advised to regularly monitor any statements that they receive from their health plans or healthcare providers, to check for any unfamiliar healthcare services. If patients notice any healthcare services that they did not receive listed on one of these statements, they should contact their health plan or the provider.”

[Exhibit A]

35. While there is current uncertainty as to the nature and extent that Plaintiff’s and class members’ sensitive HIPAA protected medical information was compromised, the fact that the breach occurred makes it likely that their private medical information will or has already been disclosed to unauthorized third parties.

**D. HIPAA and Data Breach Liability In New York**

36. The Health Insurance Portability and Accountability Act (HIPAA), is federal legislation passed in 1996 which requires providers of health care to ensure the privacy of patient records and health information. HIPAA required the federal Department of Health and Human Services (HHS) to develop regulations to implement these privacy requirements, called the Privacy Rule, which became effective on April 14, 2003.

37. SBUH [provider] contracted with BLACKBAUD [cloud services provider or “CSP”] for communications and fundraising software services and provided BLACKBAUD with personal information concerning Plaintiff and tens of thousands of other SBUH patients, including their name, date of birth, address/contact information, attending doctor, insurance provider and medical service department.

38. The HIPAA Rules establish important protections for individually identifiable health information (called protected health information or PHI when created, received, maintained, or transmitted by a HIPAA covered entity or business associate), including limitations on uses and disclosures of such information, safeguards against inappropriate uses and disclosures, and individuals’ rights with respect to their health information.

39. Covered entities and business associates must comply with the applicable provisions of the HIPAA Rules. A covered entity is a health plan, a health care clearinghouse, or a health care provider who conducts certain billing and payment related transactions electronically. A business associate is an entity or person, other than a member of the workforce of a covered entity, that performs functions or activities on behalf of, or provides certain services to, a covered entity that involve creating, receiving, maintaining, or transmitting PHI. A business associate also is any subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

40. When SBUH, a covered entity engaged the services of BLACKBAUD, [a CSP] to create, receive, maintain, or transmit ePHI (such as to process and/or store ePHI), on its behalf, the CSP is a business associate under HIPAA.

41. Further, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit ePHI on its behalf, the CSP subcontractor itself is a business associate. This is true even if the CSP processes or stores only encrypted ePHI and lacks an encryption key for the data.

42. Lacking an encryption key does not exempt a CSP from business associate status and obligations under the HIPAA Rules. As a result, the covered entity (or business associate) and the CSP must enter into a HIPAA-compliant business associate agreement (BAA), and the CSP is both contractually liable for meeting the terms of the BAA and directly liable for compliance with the applicable requirements of the HIPAA Rules.

43. For providers such as SBUH, that are covered under HIPAA, the Privacy Rule's requirements apply to all disclosures of protected health information, regardless of the purpose for which the protected health information was created. The type of service rendered, and the existence of a provider-patient relationship are irrelevant in determining if the requirements of

the Privacy Rule apply. Once a provider meets the regulatory definition of a healthcare provider subject to HIPAA's regulations, then that provider must comply with the Privacy Rule's requirements for all uses and disclosures of protected health information.

44. On July 25, 2019, New York Governor Andrew Cuomo signed into law the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act") amending New York's data breach notification law.

45. The SHIELD Act covers any and all persons or entities that have the private information of New York residents regardless of size or whether they are actually located in New York. It applies to for-profits and not-for-profits. Virtually every health care provider and payor in New York is already required to abide by the HIPAA and HITECH regulations covering security of personal health information, but they must become familiar with the SHIELD Act's provisions and make appropriate revisions to their data security compliance policies and procedures. Vendors and contractors with which private information is shared must also get into compliance with the SHIELD Act's requirements.

46. The SHIELD Act introduces significant changes, including.

a. The Act broadens the definition of "private information" to include biometric information and username/email address in combination with a password or security questions and answers. It also includes an account number or credit/debit card number, even without a security code, access code, or password if the account could be accessed without such information.

b. The Act expands the definition of "breach of the security of the system" to include unauthorized "access" of computerized data that compromises the security, confidentiality, or integrity of private information, and it provides sample indicators of access. Previously, a breach was defined only as unauthorized acquisition of computerized data.

c. The Act expands the territorial application of the breach notification requirement to any person or business that owns or licenses private information of a New York resident. Previously, the law was limited to those that conduct business in New York.

d. The Act requires companies to adopt reasonable safeguards to protect the security, confidentiality, and integrity of private information. A company should implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal. In order to achieve compliance, a business must implement a data security program that includes at least the following:

i. reasonable administrative safeguards that may include designation of one or more employees to coordinate the security program, identification of reasonably foreseeable external and insider risks, assessment of existing safeguards, workforce cybersecurity training, selection of service providers capable of maintaining appropriate safeguards and requiring those safeguards by contract, and a process for implementing adjustments to the security program based on business changes or new circumstances;

ii. reasonable technical safeguards that may include risk assessments of network, software design and information processing, transmission and storage, implementation of measures to detect, prevent and respond to system failures, and regular testing and monitoring of the effectiveness of key controls; and, reasonable physical safeguards that may include detection, prevention and response to intrusions, and reasonable technical safeguards that may include risk assessments of network, software design and information processing, transmission and storage, implementation of measures to detect, prevent and respond to system failures, and regular testing and monitoring of the effectiveness of key controls; and,

iii. reasonable physical safeguards that may include detection, prevention and response to intrusions, and protections against unauthorized access to or use of private information during or after collection, transportation and destruction or disposal of the information, and disposal of information after a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

47. BLACKBAUD did not comply with the SHIELD ACT and negligently failed to implement required safeguards and quality-control mechanisms to protect the security, confidentiality, and integrity of the Private Information of Plaintiff and Class members.

48. BLACKBAUD negligently failed to implement a data security program containing specific measures, including risk assessments, employee training, vendor contracts, and timely data disposal.

49. BLACKBAUD maintained and secured the Private Information of Plaintiff and Class members in a reckless manner, including, inter alia, failing to safeguard against ransomware attacks.

50. The Private Information was maintained on BLACKBAUD'S respective computer networks in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff and Class Members' Private Information was a known and acknowledged risk to BLACKBAUD, which failed to take steps necessary to timely and reasonably implement protocols, training, and adjustments to its security program to mitigate and/or prevent those risks.

**E. Plaintiff and Class Members' Damages**

51. Personal data has value. Facebook and Google harvest billions from it through advertising. Talented hackers make a handsome living from stealing and selling it. Private Information data is often easily taken because it is less protected and regulated than payment card data. It has been estimated that, on average, the personal data of a US resident is worth somewhere in the regions of \$2000-\$3000 per year.

<http://permission.io/blog/how-much-is-data-worth/>

52. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

53. Plaintiff 's Private Information was compromised as a direct and proximate result of the Data Breach. While the compromise of Ms. Faszczewski's information was known as early as May of 2020, she did not receive a Data Breach Notices until September 14, 2020. [Exhibit A].

54. As a direct and proximate result of BLACKBAUD's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

55. As a direct and proximate result of BLACKBAUD's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

56. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

57. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential

fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

58. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

59. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

60. Private Information is a valuable commodity for which a market exists and is being sold by hackers on the dark web.

61. One Law Journal has stated that the value of Personal Information is a valued commodity and financial asset:

Corporate America's increasing dependence on the electronic use of personally identifiable information ("PII") necessitates a reexamination and expansion of the traditional conception of corporate assets. PII is now a commodity that companies trade and sell. As technological development increases, aspects of day-to-day business involving PII are performed electronically in a more cost effective and efficient manner. PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.

<https://scholarship.richmond.edu/jolt/vol15/iss4/2>

62. Plaintiff and Class members have been damaged by the unauthorized disclosure of their personal information in the subject data breach and have lost the sales value of their personal information, as a proximate result.

63. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial, medical accounts and records for misuse and fraud.

64. Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of BLACKBAUD, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

65. As a result of BLACKBAUD'S wrongful conduct, Plaintiff and Class Members are forced to live with the knowledge that their Private Information—which contains the most intimate details about a person's life, may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of their right to privacy.

66. Plaintiff and Class Members are now forced for long periods of time to endure the fear of whether their Private Information will be used.

67. As a direct and proximate result of BLACKBAUD'S negligent actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

#### **CLASS ACTION ALLEGATIONS**

68. Plaintiff brings this action individually and on behalf of all other persons similarly situated ("the Class").

69. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

**All former and current patients of Stony Brook University Hospital, whose Private and HIPAA Information was compromised in the 2020 Data Breach described by BLACKBAUD at [www.blackbaud.com/securityincident](http://www.blackbaud.com/securityincident).**

70. Excluded from the Class are BLACKBAUD'S officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,



attorneys, successors, heirs, and assigns of BLACKBAUD. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

71. Plaintiff is a member of the class she seeks to represent.

72. This action has been brought and may properly be maintained as a class action against BLACKBAUD pursuant to FRCP Rule 23, because there is a well-defined community of interest in the litigation and the proposed Class is easily ascertainable.

73. Numerosity. The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, the class consists of approximately tens of thousands of persons whose data was compromised in Data Breach.

74. Commonality. Common questions of law and fact exist for the proposed class claims and predominate over questions affecting only individual class members. Common questions include:

- a. Whether Defendant owed a duty to Plaintiffs and members of the proposed classes to take reasonable measures to safeguard their Private Information;
- b. Whether Defendant knew or should have known that their systems were inadequate and susceptible to a data breach;
- c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendant's failure to implement adequate security controls violate applicable state consumer protection laws;
- e. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- f. Whether Defendant breached its legal duties in allowing its cybersecurity systems to be compromised;
- g. Whether Defendant owed a duty to Plaintiff and members of the proposed classes to provide timely and adequate notice of the data breach;

- h. Whether Defendant failed to provide notice of the Data Breach in a timely manner;
- i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;
- j. Whether Defendant's conduct was negligent;
- k. Whether Defendant's conduct was negligent per se;
- l. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's negligence and misconduct;
- m. Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.
- n. Which security procedures and data-breach notification procedure Defendant should be required to implement as part of any injunctive relief ordered by the Court.

75. Typicality. Plaintiff's claims are typical of the claims of the proposed Class because, among other things, Plaintiff and Class members sustained similar injuries as a result of BLACKBAUD's uniform wrongful conduct and their legal claims all arise from the same core data breach and business practices of Defendant.

76. Adequacy. Plaintiff will fairly and adequately protect the interests of the Class. Her interests do not conflict with class members' interests and she has retained counsel experienced in complex class action and data privacy litigation to vigorously prosecute this action on behalf of the Class.

77. Commonality. Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation.

78. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from

Defendant's conduct affecting Class Members, as described supra, predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

79. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would likely find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

80. BLACKBAUD has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

**FIRST CAUSE OF ACTION  
NEGLIGENCE  
(On Behalf of Plaintiff and All Class Members)**

81. Plaintiff incorporates the above allegations as if fully alleged herein.

82. BLACKBAUD's client, SBUH, required Plaintiff and Class Members to submit non-public Private Information in order to obtain medical care, treatment and other healthcare services. BLACKBAUD had a duty to SBUH, Plaintiff, and Class Members to securely maintain the Private Information collected.

83. By accepting the duty to maintain and secure this data in its computer property, and sharing it and using it for commercial gain, BLACKBAUD had a duty of care to use reasonable means to secure and safeguard its computer property and Plaintiff's and Class Members' Private Information held within it to prevent disclosure of the information, and to safeguard the information from theft.

84. BLACKBAUD owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, retaining, deleting, securing, and protecting their Private Information from being compromised, lost, stolen, accessed, or misused by unauthorized persons.

85. BLACKBAUD's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach and/or ransomware attack.

86. More specifically, this duty included among other things: (a) designing, maintaining, and testing BLACKBAUD's security systems to ensure that Plaintiff and class members' Private Information was adequately secured and protected; (b) implementing adequate and effective processes to detect an intrusion into their information systems in a timely manner; (c) timely acting upon warnings and alerts, including those generated by their own security systems, regarding network intrusions; and (d) maintaining data security measures at least consistent with industry standards.

87. BLACKBAUD's duty of care to use reasonable security measures arose as a result of the special relationship that existed between BLACKBAUD and its Clients and Users, which is recognized by Defendant's Policy Notice North America, as well as laws and regulations.

88. BLACKBAUD was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a ransomware attack and/or data breach.

89. BLACKBAUD had a specific duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

90. In New York, BLACKBAUD’s duty to Plaintiff and Class members also arises under the SHIELD ACT, which required BLACKBAUD to adopt reasonable safeguards to protect the security, confidentiality, and integrity of private information.

91. BLACKBAUD’s duty to Plaintiff and Class members arose not only as a result of the statutes and regulations described above, but also because Defendant is/was bound by industry standards to protect confidential Private Information.

92. BLACKBAUD also had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and class members were the foreseeable and probable victims of its inadequate security practices. It was clearly foreseeable that Plaintiff and class members would be harmed by the failure to protect their personal information, because hackers routinely attempt to steal such information and use it for nefarious purposes.

93. BLACKBAUD breached its duties and was negligent by failing to use reasonable measures to protect Plaintiff and Class Members’ Private Information. The specific negligent acts and omissions committed by BLACKBAUD include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members’ Private Information;

- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and
- f. Failing to timely notify Class Members about the Ransomware Attack so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

94. It was foreseeable that BLACKBAUD's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches in the healthcare industry.

95. As a proximate result of BLACKBAUD's negligent omissions and commissions as set forth above, Plaintiff and all Class members have sustained actual and ascertainable injury, damages and pecuniary loss as set forth in paragraphs 51-67 above.

96. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the subject Data Breach.

97. Plaintiff and Class Members are also entitled to injunctive relief requiring BLACKBAUD to (i) improve and strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**SECOND CAUSE OF ACTION  
BREACH OF EXPRESS CONTRACT  
(On Behalf of Plaintiff and All Class Members)**

98. Plaintiff incorporates the above allegations as if fully alleged herein.

99. Plaintiff and members of the Class were the direct or third-party beneficiaries of valid and enforceable express contracts, with BLACKBAUD (including, inter alia, Privacy Policy North America).

100. In fact, BLACKBAUD’S Privacy Policy North America expressly extends to any “constituent, supporter, patient or student of one of [Blackbaud’s] customers...”

<https://www.blackbaud.com/company/privacy-policy/north-america>

101. The valid and enforceable express contracts that Plaintiff, Class Members, and SBUHs entered into with BLACKBAUD include Defendant’s promise to protect Private Information given to Defendant’s Clients and otherwise maintained and secured by Defendant.

102. Under these express contracts, BLACKBAUD promised and was obligated to protect Plaintiff’s and the Class Members’ Private Information. In exchange, SBUH, Plaintiff, and members of the Class agreed to pay money for these services.

103. The protection of Plaintiff’s and Class Members’ Private Information were material aspects of these contracts.

104. At all relevant times, BLACKBAUD expressly represented in its Privacy Policy North America as follows:

While no website can guarantee exhaustive security, we maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons. We also advise all Blackbaud employees about their responsibility to protect customer data and we provide them with appropriate guidelines for adhering to our company’s business ethics standards and confidentiality policies.

105. BLACKBAUD's express representations, including, but not limited to, express representations found in its Privacy Policy, formed an express contract requiring BLACKBAUD to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

106. Consumers of healthcare and education, as well as non-profit donors, value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with healthcare, education, and other institutions private. To customers such as Plaintiff and Class Members, maintenance and security of Private Information that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than such services that adhere to industry-standard data security. Plaintiff and Class Members would not have given SBUH and BLACKBAUD their Private Information, and otherwise entered into these contracts with BLACKBAUD and/or SBUH as a direct or third-party beneficiary, without an understanding that their Private Information would be safeguarded and protected.

107. Plaintiff and members of the Class provided their Private Information to BLACKBAUD and/or SBUH, its affiliated Client, with a reasonable expectation of protection of their Private Information.

108. Plaintiff and Class Members performed their obligations under the contract, including when they paid for services provided by SBUH and/or otherwise donated money to SBUH.

109. BLACKBAUD materially breached its contractual obligation to protect the Private Information, by failing to maintain appropriate physical, electronic and procedural safeguards to "protect [its] databases with various physical, technical and procedural measures and [we]



restrict access to your information by unauthorized persons,” or otherwise adequately train employees.”

110. BLACKBAUD did not comply with industry standards, or otherwise protect Plaintiff’s and the Class Members’ Private Information, as set forth above.

111. BLACKBAUD failed to take reasonable steps to ensure that their contractors used safe and secure systems to protect that Private Information.

112. BLACKBAUD failed to ensure that their contractors had appropriate security protocols and measures in place to protect that Private Information.

113. BLACKBAUD allowed their contractors to disclose that information to unauthorized third parties.

114. BLACKBAUD failed to promptly alert or give notice of the breach to Plaintiff and class members.

115. As a direct and proximate result of BLACKBAUD’s breach of contract, Plaintiff and Class members did not get what they had bargained for; to wit, healthcare services which protected their sensitive Private Information.

116. As a result of BLACKBAUD’s failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in the contracts.

117. By reason of BLACKBAUD’s breach, Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the negligent/legally deficient data security protection services they actually received.

118. As a proximate result of BLACKBAUD's breach of contract, Plaintiff and Class members have suffered actual damages resulting from the exposure of their Private Information, Plaintiff and all Class members have sustained actual and ascertainable injury, damages and pecuniary loss as set forth in paragraphs 49-65 above.

119. Had BLACKBAUD disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, the Plaintiff, the Class Members, or any reasonable person would not have accepted or purchased services from BLACKBAUD and/or SBUH, which required providing Private Information.

120. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain.

121. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach, in an amount to be determined at trial.

**THIRD CAUSE OF ACTION  
BREACH OF IMPLIED CONTRACT  
(On Behalf of Plaintiff and All Class Members)**

122. Plaintiff incorporates the above allegations as if fully alleged herein.

123. When Plaintiff and Class Members provided their Private Information to SBUH, as a condition for receiving SBUH'S healthcare services, they entered into implied contracts with BLACKBAUD in which said Defendant agreed to reasonably protect their Private Information.

124. BLACKBAUD solicited and invited Class Members to provide their Private Information as part of Defendant's regular business practices, including through its Privacy Policy.

125. Plaintiff and Class Members accepted BLACKBAUD's offers and provided their Private Information to Defendant.

126. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that BLACKBAUD's data security practices complied with relevant laws and regulations and were consistent with industry standards.

127. Plaintiff and Class Members would not have entrusted their Private Information to BLACKBAUD in the absence of the implied contract between them and Defendant to keep their Private Information reasonably secure.

128. Plaintiff and Class Members would not have entrusted their Private Information to BLACKBAUD in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

129. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with BLACKBAUD.

130. BLACKBAUD breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

131. As a direct and proximate result of BLACKBAUD'S breaches of the implied contracts, Class Members sustained damages as alleged herein.

132. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

133. Plaintiff and Class Members are also entitled to injunctive relief requiring BLACKBAUD to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**FOURTH CAUSE OF ACTION**  
**[N.Y. GEN. BUS. LAW § 349, et. seq.]**

134. Plaintiff incorporates the above allegations as if fully alleged herein.

135. BLACKBAUD engaged in deceptive acts or practices in the conduct of its business, trade, and commerce, or furnishing of services, in violation of N.Y. Gen. Bus. Law § 899-bb, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and class members' Private Information, which was a direct and proximate cause of the subject data breach;
- b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA, 15 U.S.C. § 6801, et seq., which was a direct and proximate cause of the data breach;
- c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and class members' Private Information, including by implementing and maintaining reasonable security measures;
- d. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA, 15 U.S.C. § 6801, et seq.;
- e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and class members' Private Information; and
- f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and

subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA, 15 U.S.C. § 6801, et seq.

136. BLACKBAUD'S representations and omissions were material because they were likely to deceive reasonable consumers as well as companies who retained BLACKBAUD, including SBUH, about the adequacy of BLACKBAUD'S data security and ability to protect the confidentiality of consumers' Private Information.

137. BLACKBAUD violated the NYS Information Security Breach and Notification Act, which is comprised of section 208 of the State Technology Law and section 899-aa of the General Business Law.

138. BLACKBAUD violated General Business Law section 899-aa [2], which provides:

2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

139. N.Y. Gen. Bus. Law § 899-bb [2] provides as follows:

2. Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security,

confidentiality and integrity of the private information including, but not limited to, disposal of data.

140. N.Y. Gen. Bus. Law § 899-bb[2][d] provides as follows:

(d) Any person or business that fails to comply with this subdivision shall be deemed to have violated section three hundred forty-nine of this chapter...

141. BLACKBAUD acted intentionally, knowingly, and maliciously to violate New York's General Business Law, § 349 and recklessly disregarded Plaintiff's and class members' rights.

142. As a direct and proximate result of BLACKBAUD's deceptive and unlawful acts and practices, Plaintiff and class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of the benefit of their bargains with Defendant; and loss of value of their personal information.

143. BLACKBAUD's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including hundreds of thousands of New Yorkers affected by the data breach.

144. The above deceptive and unlawful practices and acts by BLACKBAUD caused substantial injury to Plaintiff and class members, that they could not reasonably avoid.

145. BLACKBAUD is liable to Plaintiff and Class members for compensatory damages available under New York General Business Law, § 349 et. seq.

146. BLACKBAUD is liable to Plaintiff and Class members for statutory damages available under New York General Business Law, § 349 et. seq.

147. Pursuant to New York General Business Law, § 349 et. seq., BLACKBAUD is liable to pay costs to Plaintiff and Class members, including reasonable attorney's fees.

**FIFTH CAUSE OF ACTION  
[NEGLIGENCE PER SE]**

148. Plaintiff incorporates the above allegations as if fully alleged herein.

149. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission, the unfair act or practice by companies such as BLACKBAUD of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of BLACKBAUD’s duties.

150. BLACKBAUD violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant’s conduct was particularly unreasonable given the nature and amount of personal information they obtained and stored and the foreseeable consequences of a data breach.

151. BLACKBAUD’s violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

152. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

153. The harm that has occurred here, is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and the class.

154. As a direct and proximate result of BLACKBAUD's negligence, Plaintiff and class members have been injured, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and behalf of the proposed Class, prays for judgment granting the following relief:

- a) For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;
- b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class;
- f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- g) For an award of punitive damages, as allowable by law;
- h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- i) Pre- and post-judgment interest on any amounts awarded; and
- j) Such other and further relief as this court may deem just and proper.

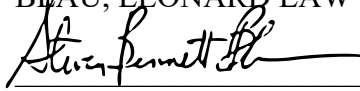


**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury of all issues in this action so triable of right.

Dated: October 5, 2020

BLAU, LEONARD LAW GROUP, LLC



---

Steven Bennett Blau

Shelly A. Leonard

23 Green Street, Suite 105

Huntington, NY 11743

(631) 458-1010

sblau@blauleonardlaw.com

sleonard@blauleonardlaw.com

*Attorneys for Plaintiff*

## **DEMAND FOR PRESERVATION**

PLEASE TAKE NOTICE that BLACKBAUD, INC. (“Defendant”), is under a legal duty to maintain, preserve, retain, protect, and not destroy any and all evidence, documents and data, both electronic and hard copy, and/or tangible items pertaining or relevant to property discoverable regarding to all of the claims made in this litigation.

This notice applies to Defendant’s on- and off-site computer systems and removable electronic media, plus all computer systems, services, and devices (including all remote access and wireless devices) used for your overall operation. This includes, but is not limited to, e-mail and other electronic communications; electronically stored documents, records, images, graphics, recordings, spreadsheets, databases; calendars, system usage logs, contact manager information, telephone logs, internet usage files, deleted files, cache files, user information, and other data. Further, this notice applies to archives, backup and disaster recovery tapes, discs, drives, cartridges, voicemail, and other data. All operating systems, software, applications, hardware, operating manuals, codes keys and other support information needed to fully search, use, and access the electronically stored information.

Electronically stored information (hereinafter “ESI”) should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, or optically stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);

- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., Zip, .GHO)

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure, or encryption utilities or devices.
- Overwriting, erasing, destroying, or discarding back up media.
- Re-assigning, re-imaging, or disposing of systems, servers, devices, or media.
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;

- Using metadata stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

In order to assure that your obligation to preserve documents and things will be met, please forward a copy of this letter to any and all persons and entities with custodial responsibilities for the items referred to herein. Notify all individuals and affiliated organizations of the need and duty to take the necessary affirmatives steps to comply with the duty to preserve evidence.

Specifically, you are instructed not to destroy, disable, erase, encrypt, alter, or otherwise make unavailable any electronic data and/or evidence relevant to potential claims and to take reasonable efforts to preserve such data and/or evidence.